Science and Technology Law Review

Volume 12 | Number 2 Article 4

2009

The Who, What, Where, When, and Why of WHOIS: Privacy and Accuracy Concerns of the WHOIS Database

Kathryn Elliott

The Who, What, Where, When, and Why of WHOIS: Privacy and Accuracy Concerns of the WHOIS Database

*Kathryn Elliott**

I. INTRODUCTION

WHOIS is a research service that provides public access to data on registered domain names, which includes the name, address, and technical information of each domain name registrant.[1] Contractual agreements specify the extent of the data collected at the time of registration of a domain name and how such data may be accessed.[2] The purpose of WHOIS is "to provide information sufficient to contact a responsible party for a particular. . .domain name who can resolve, or reliably pass on data to a party who can resolve, issues related to the configuration of the records associated with the domain name."[3] Both businesses and consumers use WHOIS information for a variety of purposes, such as researching the availability of a specific domain name to purchase or determining the owner of a particular domain name.[4]

Domain name registrars are required to collect valid data, but registrants do not always provide accurate and complete contact information.[5] The accuracy of WHOIS data is critical to law enforcement agencies, intellectual property owners, and consumers who use the contact data information to identify and locate website owners.[6] Providing false or incorrect information allows domain name registrants to commit crimes via the Internet while remaining untraceable by law enforcement agencies and governmental enti-

---

* Kathryn Elliott is a May 2009 candidate for Juris Doctor at Southern Methodist University Dedman School of Law. She graduated from Southern Methodist University with a Bachelor of Arts in Psychology, with minors in History and Political Science.

1. Jeffrey S. Sobek, Comment, *Balancing Individual Privacy Rights and the Rights of Trademark Owners in Access to the WHOIS*, 38 J. MARSHALL L. REV. 357, 358 (2004).

2. Internet Corp. for Assigned Names and Numbers Topics, *Whois Services*, http://www.icann.org/topics/whois-services (last visited May 22, 2009) [hereinafter ICANN WHOIS Services].

3. *Id.*

4. Sobek, *supra* note 1, at 362.

5. Ben Edelman, Large-Scale Intentional Invalid WHOIS Data: A Case Study of "NicGod Productions"/ "Domains for Sale," http://cyber.law.harvard.edu/people/edelman/invalid-whois (last visited May 22, 2009) [hereinafter Edelman Study].

6. Lawrence V. Molnar, *Who Owns "invisible.com," and "Whois" Disappearing? A Practitioner Looks for Answers*, 48 RES GESTAE 26, 27 (2005).

ties.[7] But despite the importance of WHOIS in identifying domain name owners, privacy advocacy groups argue that providing personal information for WHOIS violates the constitutional right to privacy, suppresses individual expression, renders Internet users vulnerable to spam and identity theft, and makes it impossible for registrants to remain anonymous.[8]

This comment will first discuss the history of the WHOIS database and explain how it is a helpful resource. The second part of this comment will focus on the current debate about the privacy and protection of contact information in the WHOIS database, as well as the Internet policies and legislation affecting the privacy and integrity of WHOIS. Third, this comment will address the latest developments in the WHOIS debate and discuss recommendations to improve the accuracy of WHOIS information while also protecting individual privacy rights.

II. WHAT IS WHOIS?

When the WHOIS service was first established in the 1970s, Internet operators used it as a source of contact information to reach computer technicians or other entities regarding operational problems with the Internet.[9] WHOIS has since evolved into a domain based research service that is used for a variety of purposes, "such as determining whether a domain name is available for registration, identifying the source of spam e-mail, enforcing intellectual property rights, and identifying and verifying online merchants."[10] The WHOIS database currently contains the name, address, and technical information of each domain name owner; this contact information is useful for fixing technical errors, holding website operators responsible for the content distributed on their websites, and resolving disputes over domain name ownership.[11]

In 1997, the U.S. Department of Commerce (DOC) was directed to transition the domain name system (DNS) to private management in such a manner that would allow for competition and international participation in DNS management.[12] The DOC selected the Internet Corporation for Assigned

7. *Id.* at 29.

8. Sobek, *supra* note 1, at 366, 368.

9. U.S. Gov't Accountability Office, Report to the Subcommittee on Courts, the Internet, and Intellectual Property House of Representatives, *Internet Management: Prevalence of False Contact Information for Registered Domain Names* 8 (2005), http://www.gao.gov/new.items/d06165.pdf [hereinafter GAO Report].

10. *Id.* at 23.

11. Edelman Study, *supra* note 5.

12. Memorandum of Understanding Between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers, http://www.ntia.doc.gov/ntiahome/domainname/icann-memorandum.htm (last visited May 22, 2009) [hereinafter MOU].

Names and Numbers (ICANN), a non-profit private corporation, to execute the transition of the joint DNS project.[13] Through a Memorandum of Understanding (MOU) with the DOC, ICANN is charged with overseeing a variety of Internet-related tasks, such as managing the assignment of domain names and monitoring the accuracy of contact information of registered domain name owners made publicly available through WHOIS.[14]

Additionally, ICANN is charged with the accreditation of domain name registrars.[15] A "registrar" is a person or entity, such as a private company, that supports registry operators by selling domain name registration services to "registrants" (the holders of specific domain names); the registrar collects information about the registrants to be made available in WHOIS.[16] Each accredited registrar is bound by the terms of the ICANN Registrar Accreditation Agreement (RAA) to maintain the WHOIS database with up-to-date, accurate contact information of all active registered domain names sponsored by the registrar.[17] The RAA also requires each registrar to make this contact data publicly available through the WHOIS service.[18]

Due to the rapidly expanding Internet, ICANN has accredited hundreds of domain name registrars worldwide.[19] These registrars compete with one another to attract and register customers, allowing the top ranking registrars to process tens of thousands of domain name registrations.[20] The domain name registration process is relatively easy for customers (registrants), who simply follow the registrar's online registration procedures.[21] The customer provides their name, address, phone number(s), and e-mail address(es), and then must confirm that they have read the registrar's registration agreement, which contains a provision requiring the customer to provide complete and accurate contact information.[22] Once the registration process is complete, the customer is the official "owner" of the domain name and can access the registrar's WHOIS database to verify the accuracy of their registration data.[23]

13. *Id.*

14. ICANN Factsheet, http://www.icann.org/en/factsheets/fact-sheet.html (last visited May 22, 2009) [hereinafter ICANN Facts].

15. Molnar, *supra* note 6, at 26.

16. GAO Report, *supra* note 9, at 17.

17. *Id.* at 21.

18. *Id.* at 22.

19. *See* Fastest Growing Registrars, http://www.webhosting.info/registrars/fastest-growing-registrars/global/?ob=rank&oo=asc (last visited May 22, 2009).

20. Molnar, *supra* note 6, at 26.

21. *Id.*

22. *Id.*

23. *Id.*

However, not all registrants correctly provide the required WHOIS contact information.[24]

A. Invalid WHOIS Information

Whether done intentionally or accidentally, incomplete and false WHOIS entries create problems for entities and individuals who search WHOIS for the contact information of domain name registrants.[25] Although registration agreements require valid contact information, some registrants provide false or incomplete data to conceal their identities or prevent contact by members of the public.[26] This is a significant issue because inaccurate and incomplete data entries inevitably produce inaccurate and incomplete WHOIS search results, making it difficult, or even impossible, to contact the correct owner of a particular domain name.[27]

By using various "tricks," registrants can conceal their identities, locations, and contact information, thus becoming untraceable through the Internet.[28] A case study of one particular domain name registrant, "NicGod Productions," revealed the different techniques used to hide its contact information.[29] NicGod registered over 1,200 domains by using eleven distinct registrars and providing at least nine different countries when registering these domains.[30] Investigations revealed that NicGod used invalid addresses and entered the name of a "few well-known individuals" as the supposed registrant of its domains (for example, "Allen Ginsberg," which is also the name of a deceased American poet).[31] Additionally, NicGod used a variety of company names in other domain registrations and has allegedly used a prior registrant's name from an existing domain as the registrant name for another domain, resulting in considerable confusion regarding who was actually responsible for NicGod's registrations.[32] It appears that NicGod has faced over twenty challenges under the Uniform Domain-Name Dispute Resolution (UDRP) but has failed to respond to any of those complaints; specifically, NicGod either chose to forfeit its domain names under the UDRP instead of revealing its identity by responding to the complaints, or it simply

24. Edelman Study, *supra* note 5.

25. Jim Wagner, False WHOIS Data Still Bedevils, http://www.internetnews.com/stats/article.php/3569521/False+WHOIS+Data+Still+Bedevils.htm (last visited May 22, 2009).

26. GAO Report, *supra* note 9, at 8.

27. *Id.* at 24.

28. Edelman Study, *supra* note 5.

29. *Id.*

30. *Id.*

31. *Id.*

32. *Id.*

did not receive the UDRP complaints as a result of the inaccurate contact information used in registration.[33]

The ease with which a registrant can provide incorrect information is problematic because "false [WHOIS] information increases the probability that the domain name owner can escape the consequences of bad behavior."[34] Although many incorrect WHOIS entries are legitimate errors on the part of registrants, other false or inaccurate entries are made by domain name owners who take advantage of anonymity to engage in illegal activities on the Internet.[35] In particular, the process for registering domain names has resulted in significant legal issues relating to identity theft, "phishing," "cybersquatting," and violations of intellectual property regulations.[36]

B. How Online Criminals Abuse WHOIS

Concerns about identity theft have significantly grown over the past few years, as have reports of identity theft, financial fraud, and security breaches.[37] The age of computers has given criminals another means of accessing and stealing personal information, such as user names, passwords, credit card numbers, and other sensitive information.[38] One method that Internet fraudsters have used to obtain personal information is a scam called "phishing," whereby e-mails and pop-up messages that appear to be from familiar businesses and organizations (banks or government agencies) are sent to unsuspecting individuals to trick them into providing their personal information.[39] The messages direct users to a webpage that appears to belong to a legitimate organization, but the website is actually controlled by the phisher, who deceives users into disclosing their personal information when they try to log into the website.[40] Using that personal information, a fraudster can steal an individual's identity and commit crimes in that person's name.[41]

Phishing affects not only computer owners, but also legitimate businesses and organizations whose brand names are hijacked by phishers and used to trick individuals into responding to "spoofed" e-mails and revealing

33. *Id.*

34. Wallace Koehler, *Who Cares about WHOIS?*, SEARCHER, July 1, 2007, at 7.

35. Wagner, *supra* note 25.

36. Koehler, *supra* note 34.

37. Erin Fonte, *Who Should Pay the Price for Identity Theft?*, FEDERAL LAWYER, Sept. 2007, at 24-25.

38. *Id.* at 26.

39. Fed. Trade Comm'n, Consumer Alert, How Not to Get Hooked by a "Phishing" Scam, www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.shtm (last visited May 22, 2009) [hereinafter FTC on Phishing].

40. *Id.*

41. *Id.*

their confidential information.[42] The Anti-Phishing Working Group (APWG), whose "members have collectively shut down hundreds of phishing websites throughout the world," maintains that the majority of phishing websites are *not* taken down or removed by conventional law enforcement agencies.[43] Instead, phishing websites are usually shut down by individual computer owners, employees of the targeted institutions, and third parties, such as private security companies, that are retained by the affected companies.[44]

Accurate public WHOIS information is an effective tool for locating and communicating with domain name owners and in bringing about the rapid deactivation of thousands of phishing websites.[45] The APWG reported in May 2007 that in over eighty percent of phishing website shut-downs, public WHOIS data was used to communicate with website owners and to link fraudulently registered domains to "other bogus registrations" that are part of phishing schemes.[46] Even when fraudulent data is registered, fraudsters often use particular methods that create a pattern in the WHOIS database (i.e., using unique names, phone numbers, or e-mail addresses).[47] By tracking these information patterns, anti-phishing services and law enforcement agencies can identify which domain names are current or future phishing websites, work with registrars to connect criminal activities with particular domain name owners, and then take action to shut down the websites.[48] However, incomplete or intentionally false WHOIS information creates a challenge for those investigating active phishing sites, making the deactivation process slower and more difficult.[49]

Another legal issue affecting computer users is "spam e-mail," which is unsolicited commercial e-mail sent out by marketers to promote their products and services.[50] Many computer users find these e-mail messages "annoying and time-consuming" because these e-mails tend to clog up their

42. Anti-Phishing Working Group, What is Phishing and Pharming?, http://www.antiphishing.org/ (last visited May 22, 2009).

43. Anti-Phishing Working Group Memorandum, Issues in Using DNS Whois Data for Phishing Site Take Down 3 (2007), http://www.antiphishing.org/reports/APWG_MemoOnDomainWhoisTake-Downs.pdf (last visited May 22, 2009) [hereinafter APWG Memo].

44. *Id.*

45. *Id.* at 4.

46. *Id.* at 3.

47. APWG Memo, *supra* note 43, at 5.

48. *Id.*

49. *Id.* at 4.

50. Fed. Trade Comm'n, Facts for Consumers, You've Got Spam: How to "Can" Unwanted Email 1(2002), http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec02.pdf (last visited on May 22, 2009) [hereinafter FTC on Spam].

inboxes, while some consumers have actually lost money through fake offers or "spam scams."[51] Because the contact information of domain name registrants is publicly available through the WHOIS database, spammers can easily collect these e-mail addresses and target registrants with spam e-mail.[52] However, the GAO has reported that the WHOIS database is also helpful in identifying the source of spam e-mail.[53] For example, the FTC relies heavily upon WHOIS in conducting investigations of illegal spam messages and Internet scams.[54] In one particular investigation, the FTC used WHOIS information to identify the website operators that were being promoted in spam messages containing sexually explicit content.[55] Once the operators were identified, the FTC attacked several companies that were in violation of federal laws for illegally exposing unsuspecting computer users to graphic sexual content through spam e-mail messages.[56] Because the WHOIS database has helped the FTC identify wrongdoers and stop their illegal activities on numerous occasions, the FTC has publicly stated that accurate WHOIS data is "critical to the agency's consumer protection laws."[57]

In addition to consumers and law enforcement agencies, intellectual property (IP) owners use WHOIS data to track registrants who have accidentally or intentionally used trademarks and brand names to which the true IP owners have rights.[58] IP owners commonly incorporate their particular trademark or brand name into the domain name for their website because their products and services are easily recognized by marks and names, and because consumers look to these trademarks to distinguish the products and services of different companies.[59] However, the domain name registration process does not include a method to ensure that a requested domain name is not infringing upon an existing registered domain name or trademark, despite extensive federal laws regulating the registration of trademarks.[60] Because of this loophole, registrants have found it easy and lucrative to register domain

51. *Id.*

52. Michael S. Guntersdorfer, *Unmasking Private Domain Name Registration*, 2006 LOS ANGELES LAWYER 19, 19.

53. GAO Report, *supra* note 9, at 23.

54. Fed. Trade Comm'n, News Release, FTC Issues Statement on WHOIS Databases, http://www.ftc.gov/opa/2006/06/icann.shtm (2006) (last visited on May 22, 2009) [hereinafter FTC on WHOIS].

55. *Id.*

56. *Id.*

57. *Id.*

58. Molnar, *supra* note 6, at 28.

59. Sobek, *supra* note 1, at 363.

60. *Id.* at 363-64.

names consisting of lawfully registered trademarks that the registrants have no right to use.[61]

Domain name registrants have discovered several ways to benefit from the trademarks of legitimate IP owners.[62] "Typosquatting" is one common, and profitable, method involving the abuse of trademarks in domain names.[63] With this particular practice, trademark counterfeiters attract Internet traffic to particular websites by registering common misspellings of well-known trademarks or brand names as domain names (for example, registering "www.citibabnk.com" instead of "www.citibank.com").[64] These websites have no purpose except to draw in users and then route the traffic to other unrelated websites, whose owners will pay the registrants of the misspelled domain names.[65] Since the WHOIS database is often the only way to identity the parties responsible for these illegal domain names, it is crucial that the contact information is accurate and complete for each domain name registrant.[66] Problems arise because website owners can easily remain unidentified and can avoid liability to consumers and companies with IP rights to trademarked names and brands.[67]

C. Who Uses WHOIS?

As previously mentioned, consumers, government agencies, and law enforcement all rely on WHOIS information to identify and communicate with domain name owners.[68] In many cases, the WHOIS database is the only available tool for identifying the party responsible for a particular domain name; without WHOIS information, it would be significantly harder to determine the sources of products and services promoted on the Internet.[69] To ensure that consumers are protected from deceptive Internet practices, the FTC has worked to stop "Internet auction fraud, Internet-based pyramid schemes, websites making deceptive health claims, and websites promoting

61. *Id.*

62. *Id.* at 364.

63. Bruce A. McDonald, *Sites in Shadow: Typosquatters on the Web Don't Deserve the Mask of Anonymity*, LEGAL TIMES (June 26, 2006), *available at* http://www.schnader.com/files/Publication/dd33566d-7191-4090-9085-d2c6ccda8109/Presentation/PublicationAttachment/d14e4dda-f214-4f52-be74-680669b0152b/McDonaldSitesShadow6-06.pdf.

64. *Id.*

65. McDonald, *supra* note 63, at 2.

66. *Id.* at 1.

67. *Id.*

68. Molnar, *supra* note 6, at 27.

69. McDonald, *supra* note 63, at 1.

'get rich quick' schemes," as well as, false claims delivered through "spam, 'phishing' schemes, and sypware."[70]

The FTC has pursued legal action against several entities that take advantage of vulnerabilities in computer software to hijack the computers of Internet users and that also violate federal laws by illegally exposing innocent computer users to sexually-explicit content without providing a warning label on spam messages.[71] While accurate WHOIS information is the most useful law enforcement mechanism, sometimes even inaccurate WHOIS information can assist in identifying and locating Internet fraudsters.[72] For example, the FTC has admitted to using a registrant's false information to link several websites to each other because each registration listed the same false name in the WHOIS contact data.[73] Additionally, the WHOIS database is often the only source the FTC can use to obtain information in cases where a registrar is located in a foreign jurisdiction, since the FTC does not specifically have the authority to require foreign entities to provide such information.[74] Thus, WHOIS information, accurate or inaccurate, is critical to FTC investigations of both national and international Internet fraudsters.[75]

WHOIS data is also helpful to interested third parties, such as attorneys or IP owners, who need to communicate with registrars to request the contact information of a particular domain name owner who is conducting illegal activity on the Internet.[76] Usually, once the IP owner or attorney has accurate contact information, the website owner is sent a cease and desist letter demanding the end of the fraud or domain name abuse.[77] In some instances the domain name owner is just "a fan of a product or celebrity and doesn't have nefarious intentions," so domain name misuse can be stopped either by making a direct plea with the owner to quit using the domain name or by simply purchasing the website from the owner.[78] Some attorneys prefer to contact a website owner rather than petition an international arbitration agency or seek a lawsuit over the misuse of a domain name.[79]

70. Fed. Trade Comm'n, Prepared Statement of the FTC before the ICANN Meeting Concerning WHOIS Databases 2 (June 2006), http://www.ftc.gov/os/2006/06/P035302WhoisDatabases.pdf (last visited May 14, 2009) [hereinafter FTC Prepared Statement].

71. *Id.* at 4-5.

72. *Id.* at 5.

73. *Id.* at 6.

74. *Id.*

75. FTC Prepared Statement, *supra* note 70, at 6.

76. Molnar, *supra* note 6, at 31.

77. *Id.*

78. Lynne Marek, *Web Site Owners May Get Tougher to Find*, NAT'L L. J. (Mar. 1, 2007), *available at* http://www.law.com/jsp/article.jsp?id=1172656996106.

79. *Id.*

However, because domain name owners cannot always be reached using WHOIS information, interested third parties must "play detective" and use the Internet in other ways to locate the website owner.[80] As previously mentioned, some domain name registrants use the same false contact information during registration, creating a traceable pattern of data that third parties can use to link certain websites together and eventually identify a particular domain name owner.[81] Although it is possible to locate a domain name registrants through false WHOIS data, the use of inaccurate information is a hindrance to direct communication that ultimately is costly to IP owners, who lose money because of domain name abuse, and is dangerous to consumers, who are vulnerable to scams through fraudulent websites.[82] It is essential to resolve these disputes as quickly as possible because delays in contacting website owners result in expensive legal work and reduced policing on the Internet.[83]

Domain name registrars, who are responsible for the registration of websites, also depend on the personal information in WHOIS, especially for "administrative and billing accountability."[84] Even though registrars need accurate information, they have neither the tools nor the incentive to ensure correct WHOIS data.[85] Although the registrars' domain name registration agreements contain provisions specifically requiring correct and complete information, these agreements also "deliberately, and conveniently, excise the registrar from any responsibility in the event that false information is discovered by a third party."[86] Some registrars require would-be domain name registrants to submit a copy of a driver's license or other form of identification as part of the registration process.[87] One registrar (Register.com) requires a $200 transfer fee to conduct a thorough investigation and background check for all registration transfers.[88] However, the majority of registrars have no added measures for ensuring accurate registrations.[89] The accuracy of WHOIS data is further complicated by the various incentives for registrars to permit false or incomplete WHOIS information: (1) the costs of incorrect data do not fall on registrars but rather on law enforcement agencies, consumers, and IP owners; (2) registrars who enforce WHOIS accuracy requirements face more expenses in comparison to those who ignore accuracy

80. Molnar, *supra* note 6, at 31.

81. *Id.*

82. *See* Marek, *supra* note 78.

83. *Id.*

84. Koehler, *supra* note 34.

85. Molnar, *supra* note 6, at 30.

86. *Id.*

87. *Id.*

88. *Id.*

89. *Id.*

requirements; and (3) registrars who enforce WHOIS accuracy requirements may experience loss in revenue by losing customers to other registrars.[90] Thus, although accurate WHOIS information is useful to registrars, there are no simple procedures or clear incentives for them to enforce WHOIS accuracy requirements.[91]

III. What is the Current State of WHOIS

A. The WHOIS Debate over Privacy Rights

Currently, the WHOIS database is the focal point of an ongoing debate concerning whether to keep the personal data of domain name owners available to the public or to make it private so that the information is not freely accessible through the Internet.[92] Privacy advocacy groups argue that the current WHOIS policies requiring complete and accurate contact information seriously affect privacy because there are no appropriate measures in place for the protection of personal information.[93] On the other hand, IP owners, Internet service providers, and law enforcement agencies argue that WHOIS should remain open and public in order to identify and locate online criminals who misuse domain names and Internet addresses.[94] Efforts by both ICANN and the U.S. Congress to address each side's concerns have yet to reduce the tension of the privacy debate.[95]

1. Argument for WHOIS Privacy

Privacy advocates, including universities, public interest groups, and religious institutions, argue that ICANN's current WHOIS policies threaten freedom of expression, the right to anonymity, and individual privacy rights.[96] One particular group, IP Justice, has long argued that WHOIS contact information is a "virtual honey-pot for abuse" for online criminals and that ICANN is violating privacy laws by forcing domain name registrars to

90. Benjamin Edelman, Testimony before the U.S. House of Representatives Committee on the Judiciary: Subcommittee on Courts, the Internet, and Intellectual Property 5 (Sept. 4, 2003), http://cyber.law.harvard.edu/people/edelman/pubs/Judiciary-090403.pdf [hereinafter Edelman Testimony].

91. Molnar, *supra* note 6, at 30.

92. Victoria Shannon, *Whatsup With "Whois"? The End User*, Int'l Herald Trib., Nov. 15, 2007, at 16, *available at* 2007 WLRWLNR 22609045.

93. Elec. Privacy Info. Ctr., WHOIS Page, *Privacy and Accuracy*, http://epic.org/privacy/whois/ (last visited May 22, 2009).

94. Shannon, *supra* note 92.

95. *See id.*

96. IP Justice, ICANN Threatens Civil Rights of Website Owners: Intellectual Property Interests Govern Use of Personal Information, http://ipjustice.org/WSIS/ICANNthreat.shtml (last visited May 22, 2009) [hereinafter IP Justice Commentary].

publish personal data without the consent of registrants.[97] According to IP Justice, the disclosure of personal information through WHOIS denies the right to anonymous publishing on the Internet, thus stifling freedom of expression and freedom of the press.[98] Private advocates argue that the right to anonymity is critical to unpopular and controversial individuals who have legitimate reasons for remaining anonymous since they face possible persecution for publishing their opinions.[99] Additionally, IP Justice criticizes ICANN's WHOIS policies for disregarding privacy rights by requiring the disclosure and publication of the name, address, telephone number, and e-mail address of each domain name owner.[100] These same policies are also criticized for violating numerous international laws that protect the privacy of personal data, including laws and guidelines established by the European Union, the United Nations, and Canada.[101] Because of the importance of privacy rights of all Internet users, IP Justice has urged ICANN to make the submission of personal information for WHOIS optional instead of mandatory.[102]

Another strong participant in the WHOIS privacy debate is the Electronic Privacy Information Center (EPIC), a public interest research center that focuses on "emerging civil liberties issues" and the protection of "privacy, the First Amendment, and constitutional values."[103] EPIC has worked with ICANN by serving on the WHOIS Privacy Steering Committee, the WHOIS Task Force, and by currently representing the Non-Commercial Users Constituency on the new WHOIS Accuracy Task Force.[104] While recognizing the need for accurate WHOIS information, EPIC's position is that enforcement of accuracy requirements "has serious implications on privacy" because there are no appropriate safeguards for privacy or data protection.[105] EPIC has recommended to ICANN that a distinction be made between commercial and non-commercial domain names "in order to protect the privacy of registrants of domain names used for religious purposes, political speech, organizational speech, and other forms of non-commercial speech."[106]

97. *Id.*

98. *Id.*

99. *Id.*

100. *Id.*

101. *Id.*

102. *Id.*

103. Elec. Privacy Info. Ctr., About EPIC, http://epic.org/epic/about.html (last visited May 22, 2009).

104. Elec. Privacy Info. Ctr., WHOIS Page, Privacy and Accuracy, http://epic.org/privacy/whois/ (last visited May 22, 2009).

105. *Id.*

106. IP Justice, EPIC and NGO Letter to ICANN Board on Need for WHOIS Reform, http://ipjustice.org/wp/2007/10/30/epic-ngo-letter-to-icann-board-on-

Privacy advocate groups base their argument for greater WHOIS privacy on the First Amendment to the U.S. Constitution, which guarantees freedom of expression in order to promote public debate and to protect the rights of controversial speakers.[107] By requiring individuals to provide personal information during the domain name registration process, privacy advocates argue that ICANN's policies "threaten a number of fundamental freedoms, such as freedom of expression, the right to anonymity, freedom of association, and individual privacy rights."[108] U.S. federal courts have recognized that the First Amendment protects anonymous speech, including speech on the Internet, so as to prevent the government from stifling expression through forced public identification of speakers.[109] Compelled public identification discourages controversial or unpopular speakers from expressing their opinions by "exposing them to harassment or retaliation for the content of their speech."[110] In recognizing that the Internet is a "valuable forum for robust exchange and debate," courts have also acknowledged that the right to speak anonymously is a critical element of Internet speech because "'Internet anonymity facilitates the rich, diverse, and far ranging exchange of ideas.'"[111]

Privacy advocates have raised other privacy considerations concerning the WHOIS database, such as mass solicitation and individual targeting.[112] The mass solicitation argument is founded on the fact that companies or individuals collect WHOIS contact information to use for mass marketing purposes like spam, telemarketing, and mass mailings.[113] The issue of individual targeting is based upon various concerns about the use of contact data to target particular individuals for criminal activities like stalking and identity theft.[114] EPIC argues that under current WHOIS policy, "anyone

need-for-whois-reform/ (last visited May 22, 2009) [hereinafter EPIC & NGO Letter].

107. *See* IP Justice, ICANN Policy Issue: WHOIS Data Protection & Individual Privacy, http://ipjustice.org/wp/campaigns/icann/whois/ (last visited May 22, 2009).

108. *See* IP Justice Commentary, *supra* note 96.

109. *See, e.g.*, Peterson v. Nat'l Telecomms. & Info. Admin., 478 F.3d 626, 632 (4th Cir. 2007).

110. *Id.*

111. *See, e.g.*, Best Western Int'l, Inc. v. Doe, 2006 WL 2091695 at *3 (D. Ariz. 2006) (citing Doe v. 2TheMart.com, Inc., 140 F. Supp.2d 1088, 1092 (W.D. Wash. 2001).

112. Sobek, *supra* note 1, at 368.

113. *Id.*

114. *Id.*

with Internet access has access to WHOIS data," including stalkers and spammers who use personal information for nefarious activities.[115]

2. Argument for an Open WHOIS

The other side of the WHOIS debate is made up of law enforcement agencies, IP owners, and Internet service providers.[116] They argue that ICANN must keep WHOIS information publicly accessible for the purpose of identifying and locating online criminals.[117] As previously discussed, the law enforcement agencies rely on WHOIS to investigate criminal activity on the Internet and to identify wrongdoers in order to protect consumers from deceptive practices on the Internet.[118] At a June 2006 meeting concerning the WHOIS database, an FTC representative urged ICANN to keep WHOIS "open, transparent, and accessible," stating that restricting the use of WHOIS information would significantly weaken the FTC's ability to quickly identify and stop online criminals from harming consumers.[119]

The Intellectual Property Constituency (IPC) of ICANN's Generic Names Supporting Organization (GNSO) represents intellectual property interests and ensures that these particular views are manifested in the GNSO Council's policy recommendations to the ICANN Board.[120] The IPC takes the position that access to WHOIS data is essential for the protection of the IP rights of businesses, non-profit organizations, and individuals.[121] This accessibility allows IP owners "to quickly contact the party responsible for the registration or use of a domain name that involves infringement of trademark or copyright, cybersquatting, or other illegal behavior."[122] The ability of IP owners to quickly contact the correct parties means that the problem is more promptly resolved, instead of going through arbitration based upon the Uniform Dispute Resolution Policy (UDRP) or formal legal processes.[123] But even when a case cannot be quickly resolved, the IPC argues that WHOIS

115. Elec. Privacy Info. Ctr., WHOIS Page, Comments on ICANN WHOIS Task Force: "Preliminary Task Force Report on WHOIS Services," http://epic.org/privacy/whois/comments.html (last visited May 22, 2009) [hereinafter EPIC Comment on Task Force].

116. Shannon, *supra* note 92.

117. *Id.*

118. *See* FTC Prepared Statement, *supra* note 70, at 2.

119. *Id.* at 6, 12.

120. Intellectual Prop. Constituency, Bylaws, http://www.ipconstituency.org/bylaws.htm (last visited May 22, 2009).

121. Intellectual Prop. Constituency, Statement on WHOIS Task Force Preliminary Report, http://www.ipconstituency.org/PDFs/IPC%20Statement%20on%20Whois%20TF%20011507.PDF (last visited May 22, 2009).

122. *Id.*

123. *Id.*

information is important in the service of legal process and further investigations of the alleged wrongdoer.[124]

Individual members of the IPC, such as the American Intellectual Property Law Association (AIPLA), are also active participants in the WHOIS debate.[125] AIPLA is a national bar association of IP lawyers whose members represent both IP owners and users involved either directly or indirectly in fields of law affecting IP.[126] AIPLA believes that WHOIS contact information of domain name registrants "should be widely and immediately available to the general public on an anonymous basis, for free, and with only limited restrictions on how the data can be used" because this policy has shown to be effective in "increasing public confidence in the Internet and ensuring its stability and commercial success."[127] In its comments regarding the WHOIS Task Force, AIPLA warned ICANN that changing the current open policies of WHOIS information would negatively affect IP owners by making the enforcement of IP rights more expensive and less effective.[128] AIPLA has recognized the relevance of privacy concerns but argues that these concerns are "clearly outweighed by the many more important legitimate uses for WHOIS information."[129] Restricting access to this data will weaken the rights of IP owners, facilitate online criminal conduct, and make the Internet a less reliable means for online commerce.[130]

The groups arguing to keep the current WHOIS policy, which include law enforcement, Internet service providers, and IP owners, each have their own group-specific reasons for keeping the WHOIS database accessible to the public.[131] Thus, these various entities rely on different grounds when arguing for the availability of WHOIS information.[132]

---

124. *Id.*

125. *See* Am. Intellectual Prop. Law Ass'n, Comments of the AIPLA on the Request for Comments Regarding the Preliminary Reports of the WHOIS Task Forces, http://www.aipla.org/Content/ContentGroups/Issues_and_Advocacy/Comments2/Domain_Name_Comments/WhoisComments3.pdf (last visited May 22, 2009).

126. *Id.*

127. *Id.*

128. *Id.*

129. *Id.*

130. *Id.*

131. *See, e.g.*, Sobek, *supra* note 1, at 369.

132. *Id.*

B. ICANN and Congress's RESPONSE

1. I CANN's WHOIS Policies

Since its creation in the early 1980s, WHOIS has been subject of numerous studies, discussions, and even congressional hearings.[133] It is not surprising that the WHOIS database is so carefully scrutinized, considering that it provides public access to personal contact information and is used by a wide range of individuals and entities.[134] For years, ICANN has tried to address questions regarding WHOIS through its own policy developing process.[135]

ICANN does not make laws regarding the domain name system because ICANN is not considered an "arm of any government."[136] Instead, ICANN policy is developed through a transparent "bottom-up collaborative process" that involves all necessary constituencies and stakeholders in the Internet community, including governmental input.[137] Because WHOIS affects so many individuals and organizations, ICANN conducts periodic reviews of policies concerning the WHOIS database.[138] Through this "policy development process," the task forces address specific issues, gather information, and seek input from stakeholders and public comments in order to reach a consensus on policy recommendations.[139] In the past few years, ICANN has commissioned several studies of WHOIS to examine particular issues affecting different Internet constituencies so that the interests of each constituency are heard.[140]

a. Task Force on WHOIS Accuracy and Bulk Access

The WHOIS Task Force's first report in December 2002 proposed both consensus polices and improvements in ICANN's enforcement of accuracy and bulk access obligations.[141] The Task Force made several policy recommendations, such as: (1) requiring registrars to remind registrants that the use of false WHOIS data could result in the cancellation of their domain name registration, and (2) eliminating the use of bulk access WHOIS information

133. Milton Mueller & Mawaki Chango, Noncommercial Users Constituency, WHOIS Timeline, 1982-2007, http://www.ncdnhc.org/Whois-timeline.htm (last visited May 22, 2009).

134. *See* Molnar, *supra* note 6, at 26-27.

135. ICANN Factsheet, *supra* note 14.

136. *Id.*

137. *Id.*

138. ICANN WHOIS Services, *supra* note 2.

139. *Id.*

140. *Id.*

141. ICANN, Final Report of the GNSO Council's WHOIS Task Force Accuracy and Bulk Access, http://www.icann.org/gnso/whois-tf/report-19feb03.htm (last visited May 22, 2009).

for marketing purposes.[142] After this final report was presented in February 2003, ICANN commissioned three more task forces to investigate the collection, display, and use of information, as well as to suggest policy proposals that balance all constituency needs and interests.[143]

b. Task Force 1: Restricting Access to WHOIS Data for Marketing Purposes

The WHOIS Task Force 1 was created to focus on the technological means for restricting access to WHOIS information for marketing purposes in order to protect this information from data mining.[144] The task force found the current mechanisms insufficient to limit the amount of data mining for marketing purposes, and concluded it was not possible under the current specifications to create technical restrictions to limit WHOIS access to a specific purpose (i.e., a non-marketing purpose).[145]

c. Task Force 2: Review of Data Collected and Displayed

Launched in October 2003, Task Force 2 examined the types of data collected by domain name registrars and displayed in WHOIS.[146] The task force recommended several changes to the current WHOIS policy, such as: (1) conducting further research on the use of "proxy registration services" provided by domain name registrars, and (2) the possibility of implementing a "tiered access" system that would provide "different data sets for different uses."[147] The task force suggested that a tiered access system would be a useful mechanism for balancing the privacy rights of domain name registrants and the need of other members of the Internet community to contact those registrants.[148]

---

142. *Id.*

143. Sheldon Burshtein, *Whazup with the WHOIS?*, 4 Can. J.L. & Tech. 77, 77 (2005), *available at* http://cjlt.dal.ca/vol4_no1/pdfarticles/burshtein.pdf.

144. ICANN, WHOIS Task Force 1 Restricting Access: Description of Work, http://gnso.icann.org/issues/whois-privacy/tor.shtml (last visited May 22, 2009).

145. ICANN, WHOIS Task Force 1 Restricting Access of Whois for Marketing Purposes: Preliminary Report 3-4, http://gnso.icann.org/issues/whois-privacy/Whois%20TF%201%20-%20Preliminary%20Report%20V2.%201.0.pdf (last visited May 22, 2009).

146. Burshtein, *supra* note 143, at 78.

147. *Id.*

148. *Id.*

d. Task Force 3: Improving Accuracy of Collected Data

Task Force 3 considered ways to improve the quality and accuracy of contact data collected during the registration process.[149] The task force recommended, among other things, that ICANN should: (1) specifically investigate registrar data collection and protection practices; (2) request direct input from each registrar regarding its current level of compliance with existing contractual agreements and its specific plans to improve the accuracy of WHOIS information it collects; (3) require domain name registrants to annually update and correct WHOIS information; (4) consider requiring domain name registrars to verify at least two out of three data elements provided by registrants (phone, fax, and e-mail); and (5) develop and execute a graduated scale of sanctions levied against parties that violate their contractual obligations.[150]

e. Task Force on the Purpose of WHOIS and of the WHOIS Contacts

In March 2006, the WHOIS Task Force released a final report on WHOIS's purpose and contacts.[151] Because the task force could not come to a consensus on the purpose of WHOIS, it produced two working formulations of the purpose of WHOIS and then invited public comments on the formulations to help the task force reach a decision.[152] In April 2006, the GNSO Council proposed that the WHOIS Task Force use the following definition:

> The purpose of the gTLD WHOIS service is to provide information sufficient to contact a responsible party for a particular gTLD domain name who can resolve, or reliably pass on data to a party who can resolve, issues related to the configuration of the records associated with the domain name within a DNS nameserver.[153]

149. ICANN, WHOIS Task Force 3 Improving Accuracy of Collected Data: Description of Work, http://gnso.icann.org/issues/whois-privacy/tor3.shtml (last visited May 22, 2009).

150. ICANN, WHOIS Task Force 3 Improve the Accuracy of Data Collected From gTLD Registrants: Preliminary Report, http://gnso.icann.org/issues/whois-privacy/Whois-tf3-preliminary.html (last visited May 22, 2009).

151. ICANN, Final Task Force Report on the Purpose of WHOIS and of the WHOIS Contacts, http://gnso.icann.org/issues/whois-privacy/tf-report-15mar06.htm#0.1 (last visited May 22, 2009).

152. *Id.*

153. ICANN, Whois Services: Background Material, https://st.icann.org/lite/page/alac-docs/statement_on_whois_hypothesis_working_group_studies_al_alac_st_0908_3 (last visited May 22, 2009).

f. WHOIS Task Force on WHOIS Services

In March 2007, the most recent WHOIS Task Force published its final recommendations for the WHOIS service.[154] The policy recommendation submitted by the Task Force, the "Operational Point of Contact" (OPoC) proposal, provided a solution to the illegal activities stemming from the amount of data that registrars are required to display in the WHOIS database.[155] Under the OPoC proposal, registrants would be required to use an OPoC instead of the current administrative and technical contact information listed in the WHOIS database.[156] Registrants would only be allowed to publish the OPoC contact information; thus, if an issue arose regarding a particular domain name the OPoC would contact the original registrant.[157]

2. Legislation of Congress

Even though ICANN oversees the domain name system and WHOIS contact information collection, the United States Congress has been significantly involved in the WHOIS-privacy debate by conducting hearings and commissioning studies on the accuracy and uses of the WHOIS database.[158] Because of the importance of this data to law enforcement in investigating spam, IP misuse, and Internet fraud, Congress asked the Government Accountability Office (GAO) to examine the extent of false WHOIS information being provided to domain name registrars.[159] Congress responded to these hearings and studies by enacting legislation to address the problems of WHOIS.[160]

a. The Anticybersquatting Consumer Protection Act

In 1999, Congress passed the Anticybersquatting Consumer Protection Act (ACPA) in an effort to resolve the problem of cybersquatting.[161] The purpose of ACPA was:

154. ICANN, Final Task Force Report on WHOIS Services, http://gnso.icann.org/issues/whois-privacy/whois-services-final-tf-report-12mar07.htm#_Toc161480256 (last visited May 22, 2009).

155. *Id.*

156. *Id.*

157. *Id.*

158. Cybertelecom, WHOIS Page: Hearings, http://www.cybertelecom.org/dns/whois.htm (last visited May 22, 2009).

159. James Bikoff & Patrick Jones, *Government Report Finds Prevalence of False Contact Information in Registered Domain Names*, IP LITIGATOR, Mar.-Apr. 2006, at 1, *available at* http://www.accessmylibrary.com/coms2/summary_0286-14406847_ITM?.

160. Burshtein, *supra* note 143, at 79.

161. Cybertelecom, DNS: US: Anti-Cybersquatter Protection Act, http://www.cybertelecom.org/dns/acparef.htm (last visited May 22, 2009).

> To protect consumers and American businesses, to promote the growth of online commerce, and to provide clarity in the law for trademark owners by prohibiting the bad-faith and abusive registration of distinctive marks as Internet domain names with the intent to profit from the goodwill associated with such marks – a practice commonly referred to as "cybersquatting."[162]

The ACPA was designed to improve the legal remedies available to trademark owners and to prevent cybersquatters from registering domain names containing American trademarks in order to extort money from those trademark holders in exchange for releasing the domain names.[163] Under the ACPA, trademark owners have more power when enforcing their IP rights online, but inaccurate information in the WHOIS database hinders their ability to identify and locate the parties infringing upon their trademarks.[164] Therefore, the lack of an effective, accurate mechanism to identify and locate infringers prevents the sufficient protection of trademarks on the Internet.[165]

b. The Fraudulent Online Identity Sanctions Act

Congressional hearings conducted in 2001, 2002, and 2003 examined the accuracy of the WHOIS database as well as the issues regarding privacy and intellectual property.[166] In 2003, representatives from the FBI and the FTC testified to Congress that law enforcement agencies relied heavily on the WHOIS database in identifying and locating criminals, but that their investigations were negatively affected by the inaccurate and incomplete WHOIS information.[167] In response to the concerns regarding WHOIS inaccuracies, Congress passed the Fraudulent Online Identity Sanctions Act (FOISA) in 2004.[168] Although the law did not make it illegal to provide false information to domain name registrars, FOISA increased prison sentences for individuals who provide false contact data to registrars and then use the reg-

162. *Id.* (quoting Senate Report No. 106-140, The Anticybersquatting Consumer Protection Act at 4 (1999)).

163. *Id.*

164. Sobek, *supra* note 1, at 365.

165. *Id.*

166. Cybertelecom, WHOIS Page: Hearings, *supra* note 153.

167. Fed. Bureau of Investigation, Congressional Testimony Page, *Testimony of James E. Farnan Before the House Judiciary Subcommittee: Subcommittee on Courts, the Internet, and Intellectual Property* (Sept. 4, 2003), http://www.fbi.gov/congress/congress03/farnan090403.htm (last visited May 22, 2009) [hereinafter FBI Testimony].

168. Angela Davids, *Fraudulent Online Identity Sanctions Act: Empowering Law Enforcement or Limiting Privacy?*, 5 IEEE COMPUTER SOC'Y (April 2004), *available at* http://www2.computer.org/portal/web/csdl/abs/html/mags/ds/2004/04/o4003.htm.

istered website in committing a felony through trademark or copyright infringement.[169] The purpose of FOISA was to make it easier for law enforcement agencies to track down violators by imposing harsher penalties for those who conceal their identities online.[170] However, reactions to FOISA were mixed – IP groups supported Congress' efforts to promote accuracy and reliability in WHOIS, while domain registrars and public interest groups opposed the law for failing to address the overall problems with WHOIS and for conflicting with privacy rights and freedom of speech.[171]

C. Where is WHOIS Now?

For the past several years, the WHOIS database has been criticized for being inaccurate and unreliable, as well as for making sensitive personal information available for Internet fraudsters.[172] Under pressure from critics, the ICANN Generic Names Supporting Organization (GNSO) took action in 2005 by convening a WHOIS Task Force to investigate better ways of handling the WHOIS data, while also considering the issues presented in the privacy debate.[173] In March 2007, a lack of consensus within the task force required GNSO to create a new study group to further review the task force's proposed solution.[174]

1. The Operational Point of Contact Proposal

The OPoC proposal, which is only supported by a slight majority of the task force, intended to reduce the amount of personal information made publicly available in the WHOIS database.[175] As previously mentioned, the OPoC proposal would permit domain name registrants to list third-party contact information in WHOIS rather than their own administrative and techni-

169. *Id.*

170. *Id.*

171. *See* Software & Info. Indus. Ass'n, SIIA Applauds Judiciary Committee Action on Internet Domain Name Fraud, at http://www.siia.net/press/releases/051204.pdf (last visited May 22, 2009); CircleID, Report on Reaction to FOISA, at http://www.circleid.com/posts/report_on_reaction_to_foisa (last visited May 22, 2009).

172. Nate Anderson, Faced With Clamor for WHOIS Reform, ICANN Votes to Study the Issue More, ARS TECHNICA, (Oct. 31, 2007), http://arstechnica.com/news.ars/post/20071031-faced-with-whois-reform-icann-votes-to-study-the-issue-some-more.html.

173. Marek, *supra* note 78.

174. Lynne Marek, *Debate over Confidentiality of Web Site Registration Information Continues*, IP L. & BUS. (May 22, 2007), *available at* http://www.law.com/jsp/article.jsp?id=1179751698776.

175. *Id.*

cal contact data.[176] The third party, an "operational point of contact," would be responsible for resolving operational matters and passing on information to the actual website owner.[177] The OPoC proposal was considered to be a compromise for those on both sides of the privacy debate because this type of system would allow website owners to keep most of their contact information confidential while still allowing the public to communicate with the domain name owner via the OPoC.[178]

However, the OPoC proposal was not accepted as a resolution to the issue of balancing privacy rights against access to website owner contact information.[179] Domain name registrars and consumer groups pushed for more privacy and confidentiality of personal contact information, while IP constituencies supported keeping as much contact data as possible publicly available.[180] OPoC faced additional hurdles because the task force could not agree on how or whether to implement OPoC, and the issue of reconciling international privacy laws with national legislation also posed challenges.[181] Adding to the intensity of the WHOIS discussion, some privacy advocates introduced a "sunset" proposal that would do away with the WHOIS database entirely.[182] The two sides of the WHOIS privacy debate could not reach an agreement on how to provide more privacy options to domain name registrants, thus, privacy advocates pushed for abolishing the current WHOIS requirements so that individuals would not have to reveal any personal information when registering for a website.[183]

Ultimately, the GNSO did not accept the task force's OPoC proposal when it voted on the matter in November 2007.[184] Representatives of domain registries, intellectual property, business, and non-commercial user constituencies voted against the OPoC proposal, consequently ending policy devel-

176. Eric Bangemen, ICANN Proposal Would Shield Contact Info in Whois Record, ARS TECHNICA, (Mar. 21, 2007), http://arstechnica.com/news.ars/post/20070321-icann-proposal-would-shield-contact-info-in-whois-record.html.

177. *Id.*

178. Marek, *supra* note 174.

179. *ICANN Registrars Feud with Business over Failed Whois Policy Talks*, WASH. INTERNET DAILY, Sept. 4, 2007, *available at* 2007 WLNR 17439235.

180. Marek, *supra* note 174, at 1.

181. *ICANN Faces Whois Debate, Cerf Departure*, WASH. INTERNET DAILY, Oct. 29, 2007, *available at* 2007 WLNR 21476235 [hereinafter Cerf Departure].

182. Anick Jesdanun, *Privacy advocates propose scrapping Whois*, THE ASSOCIATED PRESS, Oct. 29, 2007, http://www.msnbc.msn.com/id/21532971/ [hereinafter Jesdanun Scrapping].

183. *Id.*

184. *ICANN's Council of the Generic Name Supporting Organisation. . .*, WASH. INTERNET DAILY, Nov. 1, 2007, *available at* 2007 WLNR 21851279.

opment for protecting the privacy of individual Internet users.[185] With the WHOIS issue officially removed from the GNSO's agenda, the panel voted to defer answering the question of whether to keep personal contact information available through WHOIS and instead approved a motion to conduct further studies on WHOIS.[186]

The latest development in the WHOIS debate occurred in February 2008 when the ICANN Security and Stability Advisory Committee (SSAC) submitted its own policy recommendations to the GNSO.[187] The SSAC backed the decision to conduct additional studies on WHOIS and made several recommendations: (1) the GNSO should continue current and proposed efforts to reconcile legal and privacy concerns within the existing WHOIS system; (2) ICANN should take "aggressive measures" in connection with improving the accuracy and reliability of registration data by including data guidelines in future registration agreements and provisions for penalties for those who do not observe these guidelines; (3) "the ICANN community should adopt an Internet standard directory service as an initial step toward deprecating the use of the WHOIS protocol in favor of a more complete directory service," such as IETF's Cross Registry Information Service Protocol (CRISP); and (4) ICANN should collaborate with all registry operators to prepare a timeline and transition process for converting from the current WHOIS system to a successor domain name directory service.[188]

IV. Why WHOIS Issues Need to Be Resolved

The problems with the WHOIS database have been abundantly clear for years, and the heated discussions that occurred in fall 2007 only emphasized the need for a solution to the current WHOIS system.[189] ICANN has spent several years studying and discussing WHOIS but has yet to come up with a proposal that satisfies and balances the needs of privacy advocates, as well as IP owners and law enforcement agencies.[190] The decision to conduct further WHOIS studies was a relief to frequent users of the WHOIS database who wanted to maintain the status quo, but it frustrated many ICANN members

185. *Id.*

186. Alex Veiga, *Whois Studies Approved, Privacy Deferred*, The Associated Press, Nov. 1, 2007, *available at* http://redmondmag.com/news/article.asp?EditorialsID=9206.

187. ICANN Sec. & Stability Advisory Comm., SSAC Comment to GNSO Regarding WHOIS Studies 1 (Feb. 7. 2008), http://www.icann.org/committees/security/sac027.pdf [hereinafter SSAC Comment].

188. *Id.* at 2.

189. *See* Veiga, *supra* note 186, at 1.

190. Jaikumar Vijayan, *Stalemate Continues on Hiding WHOIS Info*, Computerworld, Sept. 17, 2007, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=302552.

and privacy advocates who wanted to see the problems of WHOIS addressed and resolved.[191]

A. What is Wrong with WHOIS?

As previously mentioned, the main problem with WHOIS is that the database contains a large amount of information that is inaccurate or incomplete.[192] This flaw in the WHOIS system is frequently taken advantage of by domain name registrants for both legitimate and illegitimate purposes.[193] Although the registration agreements require domain name registrants to provide complete and accurate contact information, the registration process is essentially an "honor system" which makes it easy for some registrants to violate the rules and regulations in the registration agreement.[194] Very few registrars actually research and check the information a customer provides during the registration process because registrars have neither the means nor the incentive to ensure accurate WHOIS information, and because registration agreements release registrars from any liability if a third party discovers false data in the system.[195]

Without procedures for determining the validity of contact information, it is difficult for registrars to enforce accuracy requirements.[196] As a result, the WHOIS database contains a significant number of invalid contact information.[197] A 2005 study by the Government Accountability Office (GAO) determined the prevalence of "patently false" and incomplete contact information in the WHOIS database.[198] "Patently false" data consisted of data that "appeared obviously and intentionally false without verification against any reference data," for example, "(999) 999-9999" for a phone number and "XXXXX" for a postal code.[199] Test results revealed that 2.31 million (5.14 percent) domain names had been registered with patently false contact information in one or more of the required WHOIS contact fields.[200] Additionally, the study found that 1.64 million (3.65 percent) domain names contained incomplete information in at least one of the required contact information fields.[201] These statistics indicate that the registration of invalid

191. *See* Veiga, *supra* note 186, at 1-2.

192. GAO Report, *supra* note 9, at 24-28.

193. Edelman Testimony, *supra* note 90, at 2.

194. Molnar, *supra* note 6, at 27.

195. *Id.* at 30.

196. Edelman Testimony, *supra* note 90, at 2.

197. *Id.* at 1.

198. GAO Report, *supra* note 9, at 9.

199. *Id.* at 25.

200. *Id.* at 27.

201. *Id.* at 28.

WHOIS information is a widespread issue that ICANN needs to address, especially because there is an association between intentionally invalid WHOIS data and other controversial activities, like spam e-mails and trademark abuse.[202]

However, while some correlation exists between intentionally false WHOIS data and illegal and fraudulent online behavior, law abiding citizens also provide intentionally inaccurate contact information in order to protect their privacy and avoid spam e-mails and online harassment.[203] A 2007 survey found that sixty-one percent of Americans said they were "very or extremely concerned" about the privacy of their personal information when shopping online, an increase from forty-seven percent in a 2006 survey.[204] These concerns are legitimate, as the Identity Theft Resource Center listed that more than 125 million personal records were reported as compromised due to data breaches in 2007, a significantly larger amount than the nearly 20 million records reported in 2006.[205] Based upon these figures and the current lack of WHOIS privacy safeguards, it is not surprising that individuals attempt to protect their privacy and security by registering inaccurate contact information in the WHOIS database.[206] Therefore, before ICANN can ensure the accuracy of WHOIS, it needs to implement methods for protecting the privacy of all WHOIS data.[207]

B. Why WHOIS Policies Are Not Working

ICANN regulates the domain name registration process, which includes enforcing the terms of its accreditation agreements with registrars.[208] These contracts require registrars to collect accurate registrant contact information, but under current ICANN policies, registrars do not have any procedures to ensure the contact information is accurate and complete.[209] Currently, ICANN has yet to either aggressively enforce these contracts or revoke any registrar's accreditation, and thus, registrars who collect invalid contact in-

202. Edelman Testimony, *supra* note 90, at 3.

203. Marek, *supra* note 174, at 1-2.

204. Anick Jesdanun, *Internet Privacy Concerns Rising, Study Finds*, THE ASSOCIATED PRESS, Jan. 16, 2008, http://www.msnbc.msn.com/id/22685515 [hereinafter Jesdanun Study].

205. *Id.*

206. Elec. Frontier Found., HR 3754: Concerns with Fraudulent Online Identity Sanctions Act, http://w2.eff.org/Privacy/Anonymity/Fraudulent_Online_Identity_Sanctions_Act/.

207. *See* Jonathan Robinson, *Solving the WHOIS Dilemma*, MANAGING INTELLECTUAL PROP., Mar. 2004, 4, *available at* www.managingip.com/Article/1255455/Solving-the-WHOIS-dilemma.html.

208. Molnar, *supra* note 6, at 34.

209. *Id.* at 30.

formation face no penalty.[210] The registration of inaccurate data and the failure of ICANN and registrars to ensure valid information have resulted in an unreliable WHOIS database that provides little help to those searching for *correct* contact information of a website owner.[211]

1. Lack of Accountability and Due Process Problems

ICANN's failure to enforce registration agreements, and the fact that users are not required to provide their information when performing a WHOIS search "results in a system that is completely lacking accountability."[212] This lack of accountability means that there is no check on WHOIS abuse or on violations of privacy and trademark rights.[213] Additionally, a system without accountability raises due process issues because a lawsuit cannot be brought against an anonymous fraudster if a plaintiff cannot serve notice of the suit.[214] However, wronged individuals still attempt to bring so-called "John Doe lawsuits" against anonymous Internet wrongdoers, even though these cases involve only one known party.[215] "John Doe lawsuits" raise concerns for federal courts, especially where the plaintiff asserts jurisdiction based on diversity of citizenship, because of the "very troubling possibility that the court could order John Doe unmasked, simply to discover that . . . there was no diversity, and that the court acted without subject matter jurisdiction."[216]

Although it is possible to bring a lawsuit against an unidentified defendant for allegedly conducting nefarious activities on the Internet, plaintiffs in John Doe lawsuits have the additional burden of trying to determine the identity of the wrongdoer who has remained anonymous through either providing inaccurate WHOIS information or privately registering the domain through an intermediary or proxy.[217] Since anonymity prevents service of legal process upon the actual wrongdoer, a plaintiff must attempt to subpoena the parties (usually registrars, domain name intermediaries, and Internet service providers) who have the wrongdoer's contact information in order to compel them to reveal the wrongdoer's identity.[218] Plaintiffs' motions seeking leave to subpoena certain parties for the wrongdoer's personal information have received varying treatment in different courts, and thus, there is no guarantee

210. *Id.* at 34.

211. *Id.*

212. Sobek, *supra* note 1, at 371.

213. *Id.*

214. *Id.*

215. *See, e.g.*, McMann v. Doe, 460 F. Supp. 2d 259, 264 (D. Mass. 2006).

216. *Id.*

217. *Id.* at 262-63.

218. *Id.*

that a plaintiff will be able to obtain the wrongdoer's contact information in order to continue the lawsuit.[219]

2. Jurisdictional Issues

The Anticybersquatting Consumer Protection Act (ACPA) was Congress' attempt to resolve the due process issue of bringing a lawsuit against an unidentified domain name registrant in trademark infringement cases concerning domain name abuse.[220] An *in rem* provision under the ACPA allows a plaintiff to request the court to transfer a domain name even if the plaintiff could not locate the registrant or if the registrant was not subject to the jurisdiction of U.S. courts.[221] However, this new *in rem* cause of action has created some controversy because "anonymous defendants who are non-U.S. residents are technically beyond the jurisdiction of a United States court."[222] Decisions by courts in these cases have been enforced, but due to international controversy, the enforcement of judgments in these lawsuits has been at best problematic, and at worst, impossible.[223]

C. Why the Privacy Debate is Not Over

Since ICANN ultimately rejected the OPoC proposal last fall and decided to keep WHOIS open while conducting further studies on the issue, the debate over WHIOS privacy has yet to be resolved.[224] ICANN's decision was a relief to frequent users of WHOIS, including law enforcement officials and IP lawyers, because the current open WHOIS system will remain in effect until further studies are conducted.[225] However, it appears that the privacy debate is far from over, and those affected by the WHOIS debate will continue to clash because neither side has proposed a workable solution.[226]

1. Privacy Advocates Want More Protection

As previously discussed, privacy advocates argue that domain name owners should be allowed to keep their contact information confidential be-

219. *See, e.g., id.* at 264; Best Western Int'l, Inc. v. Doe, 2006 WL 2091695, at *6-7 (D. Ariz. 2006).

220. Sobek, *supra* note 1, at 372.

221. A. Michael Froomkin, *The Collisions of Trademarks, Domain Names, and Due Process in Cyberspace*, COMMC'NS OF THE ACM, Feb. 2001, at 94, http://delivery.acm.org/10.1145/360000/359236/p91froomkin.pdf?key1=359236&key2=9864374021&coll=GUIDE&dl=GUIDE&CFID=57929956&CFTOKEN=87231847.

222. Sobek, *supra* note 1, at 372.

223. *Id.*

224. *See* Veiga, *supra* note 186.

225. *Id.*

226. *Id.*

cause anonymity promotes freedom of speech and protects users from fraudulent Internet activity.[227] Although these concerns are valid, a closed WHOIS database is not the proper solution because many WHOIS users, such as law enforcement officials, IP owners, IP attorneys, and individual consumers, have legitimate purposes for seeking the contact information of domain name owners.[228] Lack of access to WHOIS information would make it more difficult for trademark owners to stop the abuse of registered trademark in domain names, for the FTC to identify and locate an individual sending out illegal spam messages, and for consumers to directly resolve problems with websites and online merchants.[229] Privacy is important, but so is stopping illegal activity on the Internet.

Some privacy advocacy groups support the OPoC proposal, as it would replace publicly available contact information with an intermediary contact that would be responsible for sending messages to the actual domain name owner.[230] These groups have stated that while the OPoC proposal is not an ideal solution to the privacy issue, it is "a starting point" that would address the concerns of privacy and accuracy of the different stakeholders.[231] While OPoC is a "compromise" for privacy advocates who would prefer even more privacy, this proposal is more tolerable than the recommendation to abandon the WHOIS database entirely since there are a number of legitimate reasons for using WHOIS contact information.[232] The argument could be made for protecting contact information of non-commercial registrants so the data is not publicly accessible, but WHOIS information of commercial websites should not be restricted from public access.[233] The owners of commercial websites do not have the same privacy rights as individuals, and the public must have the ability to identify and communicate with businesses. Therefore, the contact information for commercial websites must remain available through WHOIS.[234]

2. IP and Law Enforcement Groups Want an Open WHOIS

Of course, the other side of the debate wants to maintain as much disclosure of WHOIS information as possible.[235] Law enforcement agencies along with IP owners and lawyers argue that WHOIS data should remain publicly available because this information is used to decrease illegal activity

227. *See, e.g.*, EPIC Comment on Task Force, *supra* note 115.

228. *See* GAO Report, *supra* note 9, at 8.

229. *See, e.g.*, FTC Prepared Statement, *supra* note 70, at 5-8.

230. EPIC & NGO Letter, *supra* note 106, at 2.

231. *Id.* at 3.

232. *See* Jesdanun, *supra* note 182, at 2.

233. *See* FTC Prepared Statement, *supra* note 70, at 9.

234. *Id.*

235. *See* Marek, *supra* note 78, at 1.

on the Internet, "whether it be the sale of counterfeit goods, the misuse of personal information by scammers and spammers or the steering of Internet traffic to pornographic sites through misuse of brand names."[236] However, an open, accessible WHOIS database that permits entities with a legitimate purpose to search for contact information also permits searches by parties with the intent to commit fraudulent or illegal activity online.[237] While this contact information is helpful to IP owners and law enforcement, the privacy and security rights of individuals also require protection.[238]

The FTC has stated that although an open WHOIS database is one of the most helpful tools available for investigating illegal online activity, the accuracy and completeness of WHOIS information could be improved through a "tiered access" system.[239] Under a tiered access system, different categories of users would have different levels of access to the information in the WHOIS database.[240] The technical and operational details as well as other basic information about the registration of a particular domain name would be anonymously available to the public, but any further information about the registrant or administrative contact would only be accessible to users in certain protected tiers.[241] As additional protection of the WHOIS information, there must be a legitimate purpose each time this protected data is accessed.[242] Several issues need addressing before a tiered access system could be implemented, but it is significant that an entity such as the FTC could potentially support such a WHOIS system that would consider the privacy interests of domain name registrants.[243] Other frequent WHOIS users would rather the contact information remain publicly accessible and in real-time, but the need for this data must be balanced against the needs for accuracy and privacy.[244]

D. International Privacy Laws

ICANN should consider international privacy laws because the requirement for domain name owners to provide their personal data for the WHOIS conflicts with privacy laws abroad that are stricter than those of the United States.[245] In countries with stricter privacy laws, such as those of the Euro-

236. *Id.* at 2.

237. IP Justice Commentary, *supra* note 96.

238. *Id.*

239. FTC Prepared Statement, *supra* note 70, at 10-11.

240. *Id.* at 11.

241. Burshtein, *supra* note 143, at 78.

242. *Id.*

243. *Id.*

244. *See* APWG Memo, *supra* note 43; FBI Testimony, *supra* note 167.

245. *See* Veiga, *supra* note 186, at 2.

pean Union, there are requirements to keep WHOIS information shielded from the public or, at minimum, domain name owners have the right to keep private their personal information, such as phone numbers and home addresses.[246] American privacy advocates argue that ICANN'S authority over WHOIS could be questioned if concerned U.S. citizens started taking lawsuits to courts with stricter privacy laws.[247]

E. What to Do Now?

The ICANN rejection of the OPoC proposal and approval of further WHOIS studies was a disappointing setback to many participants of the fall 2007 discussion, especially since ICANN had already spent the past seven years conducting studies on the WHOIS.[248] The privacy advocates and the groups supporting an open WHOIS have made it clear that the debate is not over.[249] In addition to privacy safeguards, ICANN also needs to further examine the issue of WHOIS accuracy since inaccurate data is another widespread problem.[250]

1. Privacy Recommendations

ICANN approval of the OPoC proposal would have been a step in the right direction toward protecting individual privacy rights, since there are currently no privacy safeguards for WHOIS data.[251] But even though the WHOIS will remain publicly accessible for now, domain name owners who want to keep their contact information confidential can register through a "private" or "proxy" registration process to protect their data.[252] In theory, proxy registration works the same way as in the OPoC proposal except that proxy registration is a service offered by registrars, whereas the OPoC would be standard for all registrants.[253] When registrants register for their domain names, they can choose to pay for private registration so that the registrar substitutes its own contact information instead of the registrants' data.[254] Despite the rejection of the OPoC, there are ways for domain name owners to protect their confidential information.[255] However, cybercrime is still an is-

246. Shannon, *supra* note 92, at 1.

247. Marek, *supra* note 78, at 3.

248. *See* Veiga, *supra* note 186, at 1.

249. *Id.*

250. *Id.*

251. *Id.*

252. Guntersdorfer, *supra* note 52, at 19.

253. *Id.*

254. *Id.*

255. Veiga, *supra* note 186, at 2.

sue with private registration, which is now being used by cyber squatters and trademark infringers to hide their identities.[256]

2. Accuracy Recommendations

a. Formal Directory Service

As previously mentioned the ICANN Security and Stability Committee (SSAC) made recommendations to the GNSO about improving the integrity and accuracy of WHOIS information.[257] The SSAC's main proposal was for the adoption of an Internet standard, uniform directory service that "provides authentication, data confidentiality, data accuracy and data integrity services."[258] More research is needed, but the implementation of a formal directory service that is secure and reliable and could satisfy the needs of the various Internet constituencies sounds more promising than the current system of "making do" with the available protocols and services.[259]

b. Sanctions

The accuracy of the WHOIS database is problematic because under current ICANN policies, registrars do not face any penalties for the registration of false or incomplete contact information of domain name registrants.[260] ICANN needs to take a more aggressive stance in enforcing its accreditation agreements with registrars, which require registrars to ensure the accuracy of contact information.[261] The SSAC recommended that ICANN provide guidelines and provisions for sanctions and other penalties for noncompliance in future accreditation agreements with registrars in order to improve the accuracy of registration information.[262] The threat of enforceable sanctions would theoretically encourage registrars to be more diligent in verifying registration information, which would likely result in more accurate, complete WHOIS data.[263]

V. Conclusion

Despite the shortcomings of the WHOIS database, it is a valuable tool that, at least for now, will remain open and available to the public.[264] The WHOIS discussions last fall left many Internet constituencies frustrated with

256. Guntersdorfer, *supra* note 52, at 19.

257. SSAC Comment, *supra* note 187.

258. *Id.*

259. *Id.*

260. *See* Molnar, *supra* note 6, at 30.

261. *Id.*

262. SSAC Comment, *supra* note 187, at 2.

263. *See* Edelman Testimony, *supra* note 90, at 4-5.

264. Veiga, *supra* note 186.

the lack of a workable proposal.[265] Because so many groups have an interest in the privacy and accuracy of WHOIS information, ICANN must continue to examine and develop solutions for WHOIS that are acceptable to all the Internet constituencies involved.[266]

265. *Id.*

266. *Id.*